Configurar o módulo de FirePOWER para a rede AMP ou o controle de arquivos com ASDM.

Índice

Introdução

Este documento descreve a funcionalidade avançada rede do controle de acesso da proteção do malware (AMP) /file do módulo de FirePOWER e do método para configurar-los com Security Device Manager adaptável (ASDM).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do Firewall da ferramenta de segurança (ASA) e do ASDM adaptáveis.
- Conhecimento do dispositivo de FirePOWER.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão de software running 5.4.1 dos módulos ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) e mais atrasado.
- Módulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) essa versão de software 6.0.0 da corrida e mais atrasado.
- ASDM 7.5.1 e mais atrasado.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O software/malware maliciosos pode entrar na rede de uma organização através das formas múltiplas. A fim identificar e abrandar os efeitos destes software e malware maliciosos, as características AMP de FirePOWER podem ser usadas a fim detectar e obstruir opcionalmente a transmissão do software e do malware maliciosos na rede.

Com funcionalidade do controle de arquivos, você pode escolher monitorar (para detectar), obstruir, ou permitir transferência do upload de arquivo e da transferência. Por exemplo, uma política do arquivo pode ser executada que obstrua a transferência dos arquivos executáveis pelo usuário.

Com funcionalidade da rede AMP, você pode selecionar os tipos de arquivo que você deseja monitorar sobre protocolos de uso geral e enviar SHA 256 pica, os metadata dos arquivos, ou mesmo as cópias dos arquivos elas mesmas à nuvem da inteligência do Cisco Security para a análise do malware. A disposição dos retornos da nuvem para o arquivo pica como limpo ou malicioso baseado na análise do arquivo.

O controle de arquivos e o AMP para FirePOWER podem ser configurados como uma política do arquivo e ser usados como parte de sua configuração total do controle de acesso. As políticas do arquivo associadas com as regras do controle de acesso inspecionam o tráfego de rede que está conformes condições da regra.

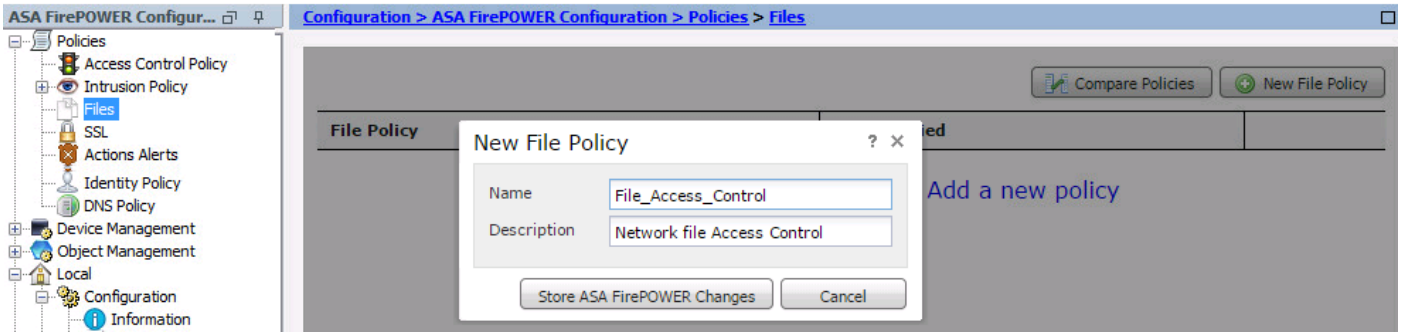
> **Note**: Assegure-se de que o módulo de FirePOWER tenha uma licença da proteção/controle/malware a fim configurar esta funcionalidade. A fim verificar as licenças, escolha a **configuração > a configuração > a licença ASA FirePOWER.**

Configurar a política do arquivo para o /Network AMP do controle de arquivos

Configurar o controle de acesso do arquivo

Entre ao ASDM e escolha a **configuração > a configuração > as políticas > os arquivos ASA FirePOWER.** A caixa de diálogo da **política do arquivo novo** aparece.

Incorpore um nome e uma descrição opcional para sua política nova, a seguir clique a opção das **mudanças da loja ASA FirePOWER**. A página da regra da política do arquivo publica-se.



O clique **adiciona a regra do arquivo** a fim adicionar uma regra à política do arquivo. A regra do arquivo dá-lhe o controle granulado sobre os tipos de arquivo de que você quer registrar, obstruir, ou fazer a varredura para o malware.

Protocolo do aplicativo: Especifique o protocolo do aplicativo como (padrão) ou o protocolo específico (HTTP, S TP, IMAP, POP3, FTP, SMB).

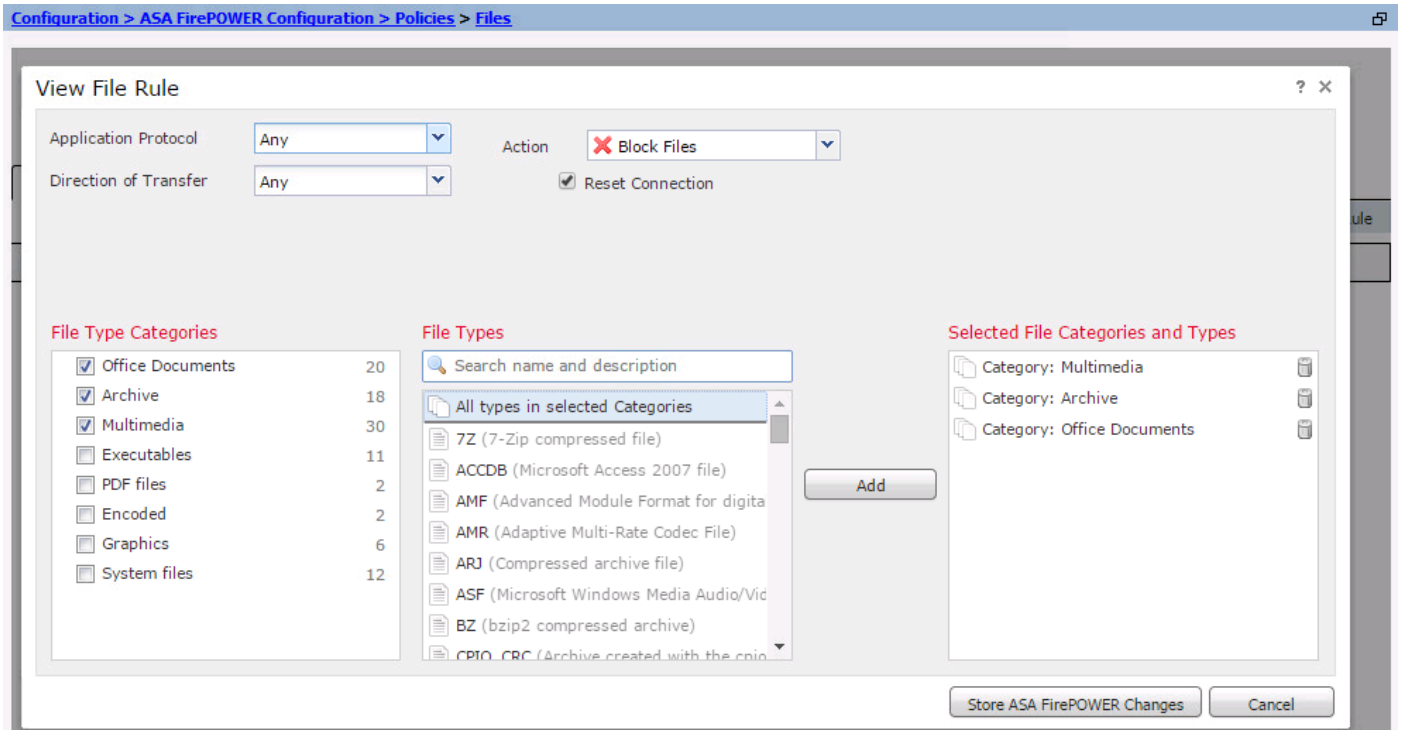
Sentido de transferência: Especifique o sentido de transferência de arquivo. Podia ser algum ou transferência de arquivo pela rede/transferência baseada no protocolo do aplicativo. Você pode inspecionar o protocolo (HTTP, IMAP, POP3, FTP, SMB) para a transferência do arquivo e o protocolo (HTTP, S TP, FTP, SMB) para o upload de arquivo. Use **toda a** opção a fim detectar arquivos sobre protocolos de aplicativos múltiplos, apesar de se os usuários enviam ou recebem o arquivo.

Ação: Especifique a ação para a funcionalidade do controle de acesso do arquivo. A ação seria **detecta arquivos** ou **obstrui arquivos. Detecte a** ação do **arquivo** gerencie o evento e a ação dos **arquivos do bloco** gerencie o evento e obstrui a transmissão de arquivo. Com ação dos **arquivos do bloco**, você pode opcionalmente selecionar **para restaurar a conexão** para terminar a conexão.

Categorias do tipo de arquivo: Selecione as categorias do tipo de arquivo para que você quer ao arquivo do bloco ou gerencie o alerta.

Tipos de arquivo: Selecione os tipos de arquivo. A opção dos tipos de arquivo dá uma opção mais granulada para escolher o tipo de arquivo específico.

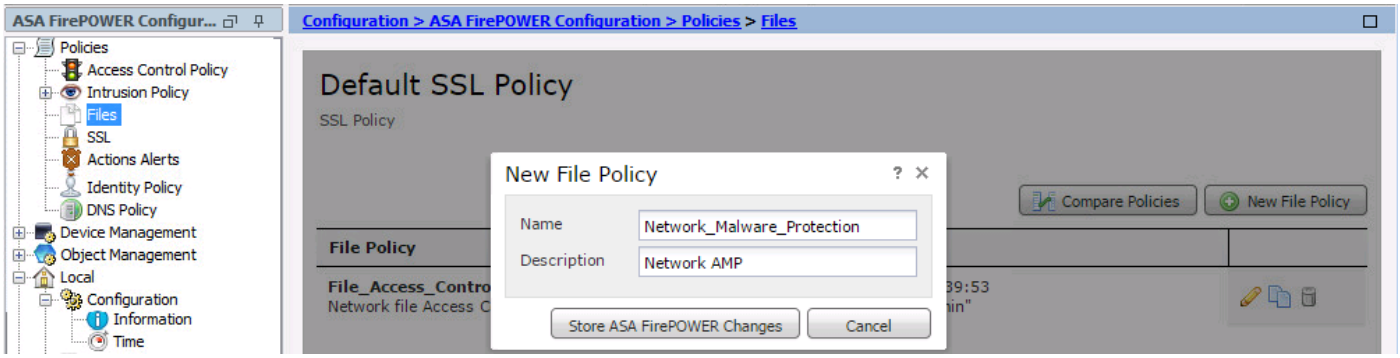
Escolha a opção das **mudanças da loja ASA FirePOWER** salvar a configuração.



Configurar a proteção do malware da rede (rede o AMP)

Entre ao ASDM e navegue à **configuração > à configuração > às políticas > aos arquivos ASA FirePOWER.** A página da política do arquivo publica-se. Clique agora sobre o a caixa de diálogo da política do arquivo novo aparece.

Incorpore um **nome** e uma descrição opcional para sua política nova, a seguir clique sobre a opção das **mudanças da loja ASA FirePOWER**. A página das regras da política do arquivo publica-se.



Clique a opção da **regra do arquivo adicionar** para adicionar uma regra para arquivar a política. A regra do arquivo dá-lhe o controle granulado sobre os tipos de arquivo de que você quer registrar, obstruir, ou fazer a varredura para o malware.

Protocolo do aplicativo: Especifique alguns (padrão) ou o protocolo específico (HTTP, S TP, IMAP, POP3, FTP, o SMB)

Sentido de transferência: Especifique o sentido de transferência de arquivo. Podia ser algum ou transferência da transferência de arquivo pela rede baseada no protocolo do aplicativo. Você pode inspecionar o protocolo (HTTP, IMAP, POP3, FTP, SMB) para a transferência do arquivo e o protocolo (HTTP, S TP, FTP, SMB) para o upload de arquivo. Use **toda a** opção para detectar arquivos sobre protocolos de aplicativos múltiplos, apesar dos usuários que enviam ou que recebem o arquivo.

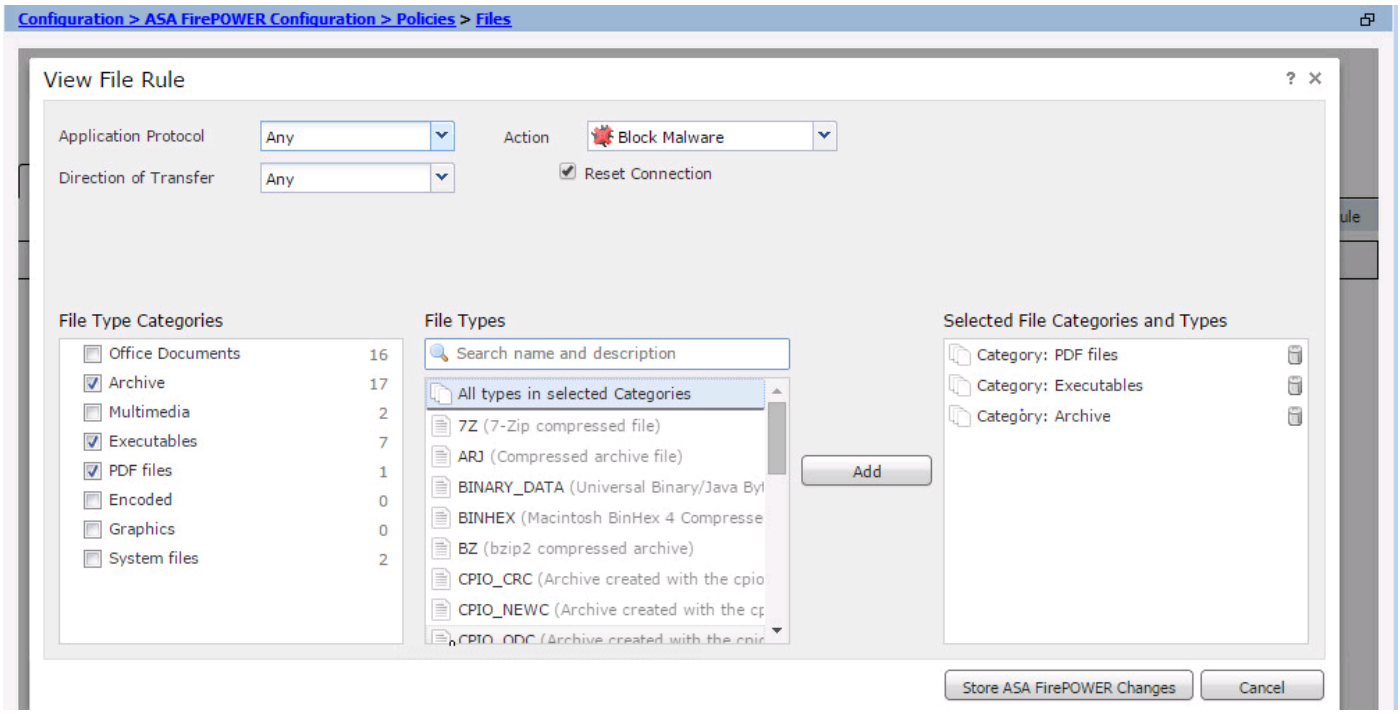
Ação: Para a funcionalidade da proteção do malware da rede, a ação seria uma ou outra **consulta da nuvem do malware** ou **obstruiria o malware. A consulta da nuvem do malware da** ação gerencie somente um evento visto que o **malware do bloco da** ação gerencie o evento assim como obstrui a transmissão de arquivo do malware.

> **Note**: As regras do **malware do** andBlock da **consulta da nuvem do malware** permitem que FirePOWER calcule a mistura do SHA-256 e envie-a para que o processo de consulta da nuvem determine se os arquivos que atravessam a rede contêm o malware.

Categorias do tipo de arquivo: Selecione as categorias específicas do arquivo.

Tipos de arquivo: Selecione os **tipos de arquivo** específicos para uns tipos de arquivo mais granulados.

Escolha **mudanças da loja ASA FirePOWER da** opção salvar a configuração.

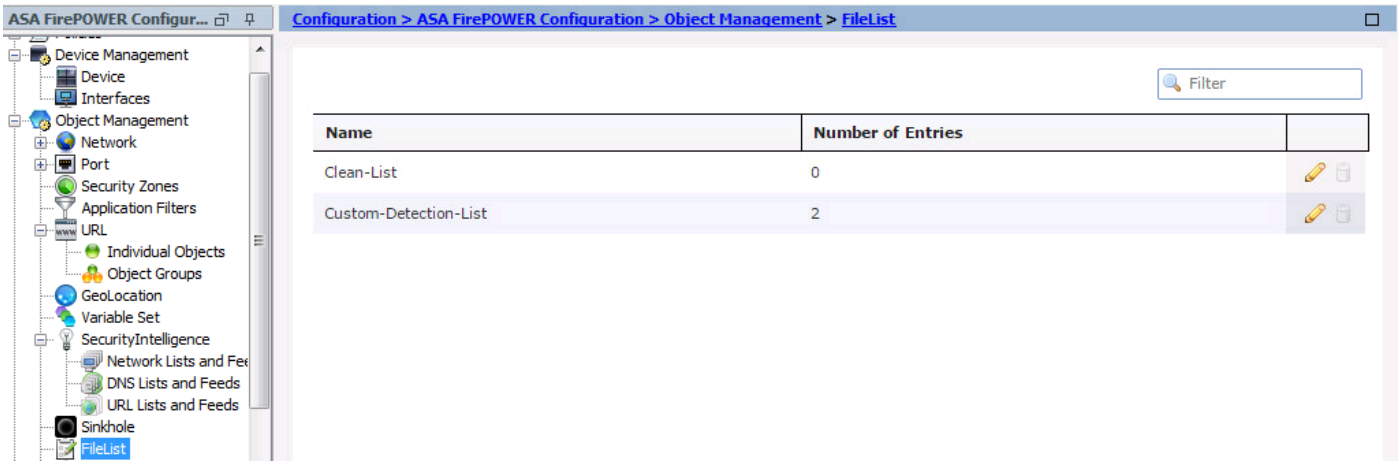


> **Note**: As políticas do arquivo seguram arquivos na seguinte ordem da regra-ação: Obstruir toma a precedência sobre a inspeção do malware, que toma a precedência sobre a detecção e o registro simples.

Se você configura a proteção avançada Com base na rede do malware (AMP), e Cisco se nubla detecta incorretamente a disposição de um arquivo, você pode adicionar o arquivo para arquivar a lista usando um valor de hash do SHA-256 para melhorar detecta a disposição do arquivo no futuro. segundo o tipo de lista do arquivo, você pode fazer:

- Para tratar um arquivo como se a nuvem atribuiu uma disposição limpa, adicionar o arquivo à lista limpa.
- Para tratar um arquivo como se a nuvem atribuiu uma disposição do malware, adicionar o arquivo à lista feita sob encomenda.

Para configurar isto, navegue à **configuração > à configuração ASA FirePOWER > ao Gerenciamento do objeto > à lista do arquivo** e edite a lista para adicionar o SHA-256.



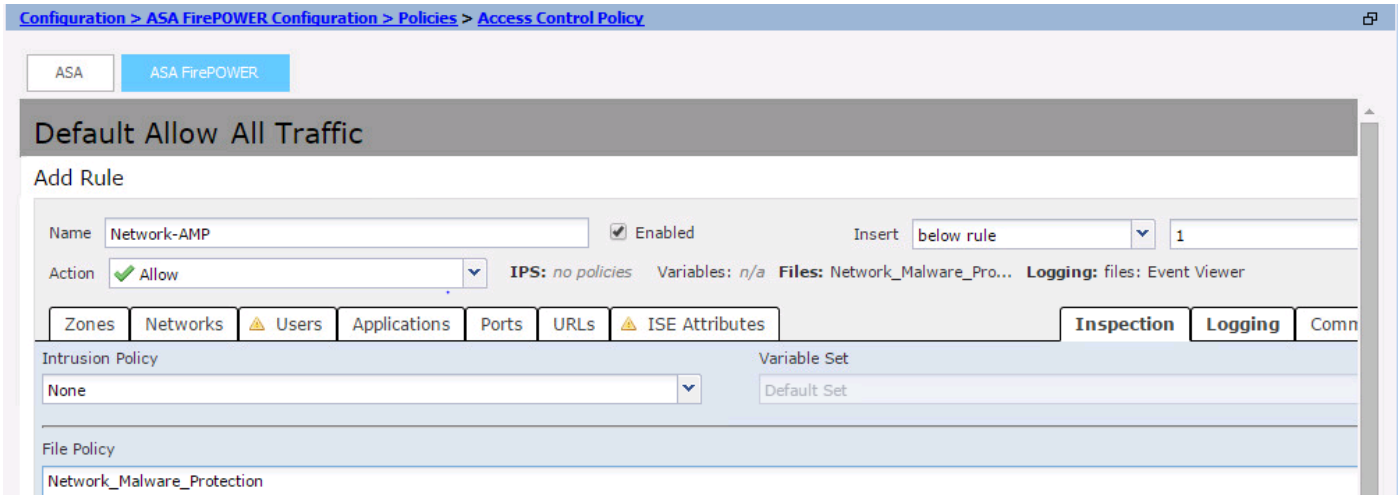
Configurar a política do controle de acesso para a política do arquivo

Navegue à **configuração > à configuração ASA FirePOWER > às políticas > à política do controle de acesso,** e crie uma ou outra **regra** nova do **acesso** ou edite **regra** existente do **acesso,** segundo as indicações desta imagem.

Para configurar a política do arquivo, a ação deve ser **reserva**. Navegue à aba da **inspeção**, e selecione a **política do arquivo do** menu de gota para baixo.

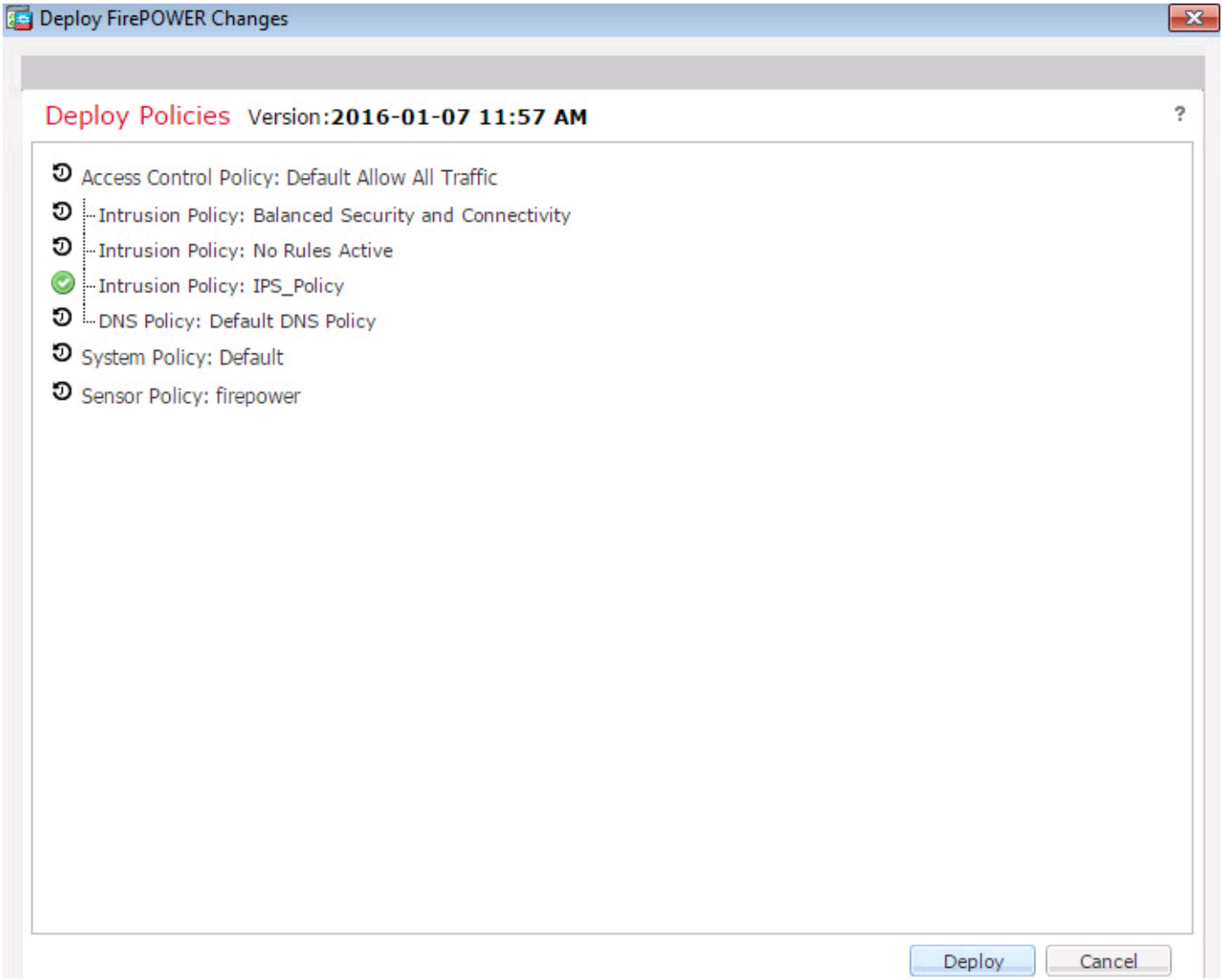
Para permitir o registro, navegue a **opção de registro**, e selecione a opção de registro & a opção apropriadas dos **arquivos de registro**. Clique a **salvaguarda/botão Add** para salvar a configuração.

Escolha **mudanças da loja ASA FirePOWER da** opção salvar as alterações de política AC.



Distribua a política do controle de acesso

Navegue aos ASDM **distribuem a** opção, e escolhem-na **distribuem a** opção da **mudança de FirePOWER do** menu de gota para baixo. Clique sobre a opção **Deploy** para distribuir as mudanças.

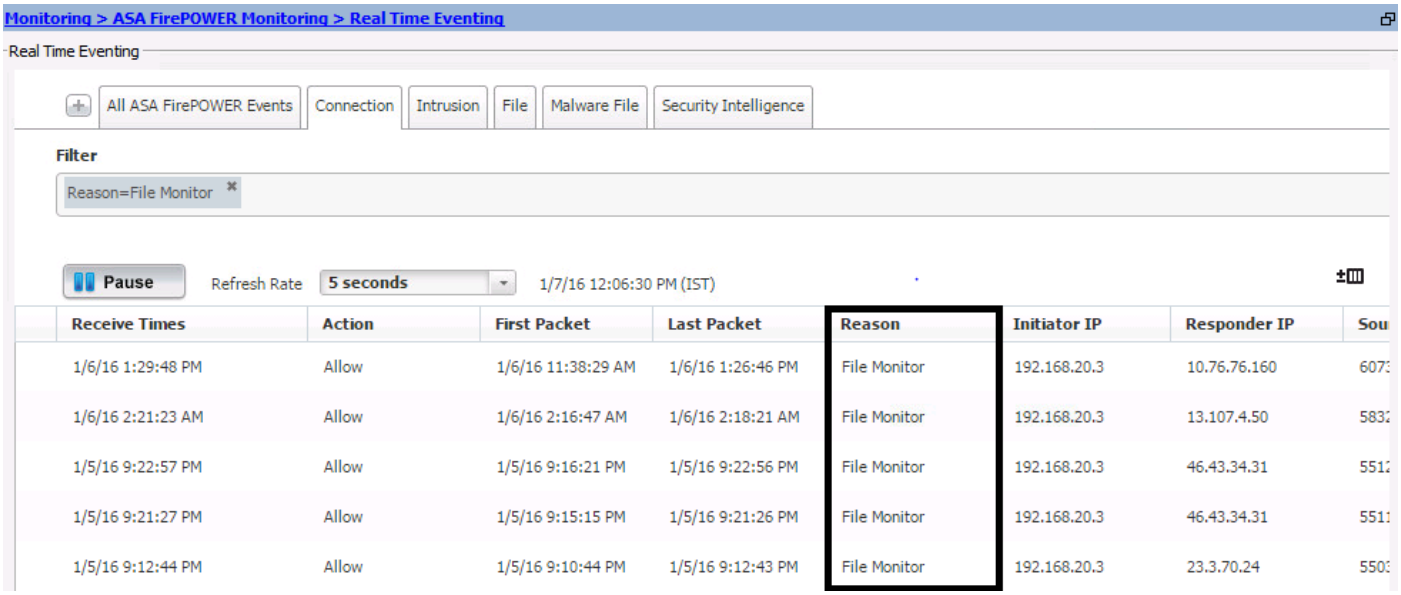


Navegue à **monitoração > ASA FirePOWER que monitora > estado da tarefa.** Assegure-se de que a tarefa deva terminar para aplicar a alteração de configuração.

> **Note**: Na versão 5.4.x, para aplicar a política de acesso ao sensor, você precisa clickApply **mudanças ASA FirePOWER.**

Monitore a conexão para eventos da política do arquivo

A fim ver os eventos gerados pelo módulo de FirePOWER relativo para arquivar a política, navegue à **monitoração > ASA FirePOWER que monitora > tempo real Eventing.**



Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Assegure-se de que a política do arquivo conifigured corretamente com tipos de arquivo da ação do sentido do protocolo. Assegure a isso a política correta do arquivo incluída em regras do acesso.

Assegure-se de que a distribuição de política do controle de acesso termine com sucesso.

Monitore os eventos dos eventos de conexão & do arquivo (**monitoração > ASA FirePOWER que monitora > tempo real Eventing**) para verificar se o fluxo de tráfego está batendo a regra correta ou não.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems